

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)



Sheet 1 of 2

Complete if Known

<b>Application Number</b>	09/540,611
<b>Filing Date</b>	March 31, 2000
<b>First Named Inventor</b>	Ellison, Carl
<b>Group Art Unit</b>	2134
<b>Examiner Name</b>	Tran, Ellen

Attorney Docket No: 42P08112

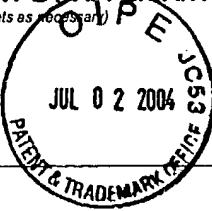
FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T <sup>2</sup>
	EP-EP0892521	01/20/1999	Zamek, Steven			
	EP-EP1055989	11/29/2000	Proudler, Graeme J., et al.			
	EP-EP1056014	11/29/2000	Proudler, Graeme J., et al.			
	WO-WO0201794	01/03/2002	Ellison, Carl			
	WO-WO02060121	08/01/2002	Grawrock, David W.			
	WO-WO03058412	07/17/2003	Glew, Andrew , et al.			
	WO-WO9812620	03/26/1998	Nishiuchi, Taiki , et al.			
	WO-WO9918511	04/15/1999	Edrich, David R.			

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
ECT		COULOURIS, GEORGE , et al., "Distributed Systems, Concepts and Designs", 2nd Edition, (1994),422-424	
		CRAWFORD, JOHN , "Architecture of the Intel 80386", <u>Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD '86)</u> , (October 6, 1986),155-160	
		FABRY, R.S. , "Capability-Based Addressing", Fabry, R.S., "Capability-Based Addressing," Communications of the ACM, Vol. 17, No. 7, (July 1974),403-412	
		FRIEDER, GIDEON , "The Architecture And Operational Characteristics of the VMX Host Machine", <u>The Architecture And Operational Characteristics of the VMX Host Machine</u> , IEEE, (1982),9-16	
		INTEL CORPORATION, "IA-64 System Abstraction Layer Specification", <u>Intel Product Specification</u> , Order Number 245359-001, (01/2000),1-112	
		INTEL CORPORATION, "Intel IA-64 Architecture Software Developer's Manual", <u>Volume 2: IA-64 System Architecture</u> , Order Number 245318-001, (01/2000),i, ii, 5.1-5.3, 11.1-11.8, 11.23-11.26	
		MENEZES, ALFRED J., et al., "Handbook of Applied Cryptography", <u>CRC Press Series on Discrete Mathematics and its Applications</u> , Boca Raton, FL, XP002165287, ISBN 0849385237,(Oct. 1996),403-405, 506-515, 570	
		NANBA, S. , et al., "VM/4: ACOS-4 Virtual Machine Architecture", <u>VM/4: ACOS-4 Virtual Machine Architecture</u> , IEEE, (1985),171-178	
		RSA SECURITY, "Hardware Authenticators", <a href="http://www.rsasecurity.com/node.asp?id=1158">www.rsasecurity.com/node.asp?id=1158</a> , 1-2	
		RSA SECURITY, "RSA SecurID Authenticators", <a href="http://www.rsasecurity.com/products/securid/datasheets/SID_DS_0103.pdf">www.rsasecurity.com/products/securid/datasheets/SID_DS_0103.pdf</a> , 1-2	
↓		RSA SECURITY, "Software Authenticators", <a href="http://www.rsasecurity.com/node.asp?id=1313">www.rsasecurity.com/node.asp?id=1313</a> , 1-2	

EXAMINER

DATE CONSIDERED

9 AUG '2004

Substitute for form 1449A/PTO <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> <i>(Use as many sheets as necessary)</i>		Complete if Known	
		Application Number	09/540,611
		Filing Date	March 31, 2000
		First Named Inventor	Ellison, Carl
		Group Art Unit	2134
		Examiner Name	Tran, Ellen
Attorney Docket No: 42P08112			
Sheet 2 of 2			

### OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No'	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T'
ECT		SCHNEIER, BRUCE , "Applied Cryptography: Protocols, Algorithm, and Source Code in C", Wiley, John & Sons, Inc., XP002939871; ISBN 0471117099,(Oct. 1995),47-52	
		SCHNEIER, BRUCE , "Applied Cryptography: Protocols, Algorithm, and Source Code in C", Wiley, John & Sons, Inc., XP002138607; ISBN 0471117099,(Oct. 1995),56-65	
		SCHNEIER, BRUCE , "Applied Cryptography: Protocols, Algorithms, and Source Code C", Wiley, John & Sons, Inc., XP0021111449; ISBN 0471117099,(Oct. 1995),169-187	
✓		SCHNEIER, BRUCE , "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition; Wiley, John & Sons, Inc., XP002251738; ISBN 0471128457,(Nov. 1995),28-33; 176-177; 216-217; 461-473; 518-522	

EXAMINER

*C. P. Tran*

DATE CONSIDERED

*12/28/04*

Substitute Disclosure Statement Form (PTO-1449)

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached



## ELECTRONIC INFORMATION DISCLOSURE STATEMENT

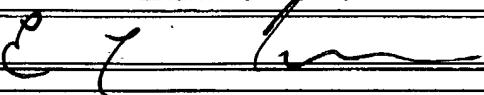
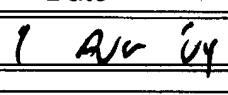
Electronic Version v18

Stylesheet Version v18.0

Title of Invention	Managing Accesses in a Processor for Isolated Execution				
Application Number:	09/540611 				
Confirmation Number:	2172				
First Named Applicant:	Carl Ellison				
Attorney Docket Number:	42P08112				
Art Unit:	2134				
Examiner:	Ellen Tran				
Search string:	( 3699532 or 4207609 or 4319233 or 4403283 or 4419724 or 5237616 or 5287363 or 5560013 or 5604805 or 5633929 or 5668971 or 5684948 or 5706469 or 5740178 or 5752046 or 5809546 or 5825880 or 5919257 or 5935242 or 5935247 or 6035374 or 6093213 or 6108644 or 6131166 or 6199152 or 6327652 or 6397379 or 6529909 or 6560627 or 6609199 or 6615278 or 6651171 or 6684326 ).pn.				
<b>US Patent Documents</b>					
Note: Applicant is not required to submit a paper copy of cited US Patent Documents					
init	Cite.No.	Patent No.	Date	Patentee	Kind
1	3699532	1972-10-17	Schaffer, Harry G., et al.		
2	4207609	1980-06-10	Luiz, Fernando A., et al.		
3	4319233	1982-03-09	Matsuoka, Michihiro , et al.		
4	4403283	1983-09-06	Myntti, Jon N., et al.		
5	4419724	1983-12-06	Branigin, Michael H., et al.		
6	5237616	1993-08-17	Abraham, Dennis G., et al.		
7	5287363	1994-02-15	Wolf, Paul I., et al.		
8	5560013	1996-09-24	Scalzi, Casper A., et al.		
9	5604805	1997-02-18	Brands, Stefanus A.		
10	5633929	1997-05-27	Kaliski, Jr., Burton S.		
11	5668971	1997-11-16	Neufeld, E. D.		
12	5684948	1997-11-04	Johnson, James S., et al.		

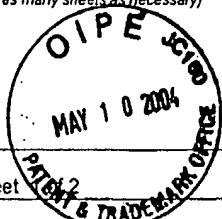
13	5706469	1998-01-06	Kobayashi, Souichi
14	5740178	1998-04-14	Jacks, Steven A., et al.
15	5752046	1998-05-12	Oprescu, Florin , et al.
16	5809546	1998-09-15	Greenstein, Paul G., et al.
17	5825880	1998-10-20	Sudia, Frank W., et al.
18	5919257	1999-07-06	Trostle, Jonathan
19	5935242	1999-08-10	Madany, Peter W., et al.
20	5935247	1999-08-10	Pai, Hsin-Ying , et al.
21	6035374	2000-03-07	Panwar, Ramesh , et al.
22	6093213	2000-07-25	Favor, John G., et al.
23	6108644	2000-08-22	Goldschlag, David M., et al.
24	6131166	2000-10-10	Wong-Isley, Becky
25	6199152	2001-03-06	Kelly, Edmund J., et al.
26	6327652	2001-12-04	England, Paul , et al.
27	6397379	2002-05-28	Yates, Jr., John S., et al.
28	6529909	2003-03-04	Bowman-Amuah, Michel K.
29	6560627	2003-05-06	McDonald, Michael F., et al.
30	6609199	2003-08-19	DeTreville, John
31	6615278	2003-09-02	Curtis, Bryce A.
32	6651171	2003-11-18	England, Paul , et al.
33	6684326	2004-01-27	Cromer, Daryl C., et al.

Signature

Examiner Name	Date
	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO  
**INFORMATION DISCLOSURE  
 STATEMENT BY APPLICANT**  
 (Use as many sheets as necessary)



Sheet 1 of 2

Complete if Known

Application Number	09/540613
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown

Attorney Docket No: 42P08628

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T <sup>2</sup>
	DE-DE4217444	12/03/1992	Toyohisa, Imada , et al.			
	EP-EP0473913	03/11/1992	Farrell, Joel A.			
	JP-JP2000076139	03/14/2000	Tanno, Masaaki , et al.			
	WO-WO0175564	10/11/2002	Herbert, Howard C., et al.	MAY 13	2004	
	WO-WO02086684	10/31/2002	Proudler, Graeme J.			
	WO-WO0217555	02/28/2002	Ford, Warwick	Technology Center 2100		

RECEIVED

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
ECF		BRANDS, STEFAN , "Restrictive Blinding of Secret-Key Certificates", SPRINGER-VERLAG XP002201306, (1995),Chapter 3
		CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999),209-221
		COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001),1-321
		DAVIDA, GEORGE I., et al., "Defending Systems Against Viruses through Cryptographic Authentication", Proceedings of the Symposium on Security and Privacy, IEEE Comp. Soc. Press, ISBN 0-8186-1939-2,(May 1989),
		IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991),156-158
		KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990),2-19
		KASHIWAGI, KAZUHIKO , et al., "Design and Implementation of Dynamically Reconstructing System Software", Software Engineering Conference, Proceedings 1996 Asia-Pacific Seoul, South Korea 4-7 Dec. 1996, Los Alamitos, CA USA, IEEE Comput. Soc, US, ISBN 0-8186-7638-8,(1996),
		LUKE, JAHN , et al., "Replacement Strategy for Aging Avionics Computers", IEEE AES Systems Magazine, XP002190614,(March 1999),
		MENEZES, OORSCHOT , "Handbook of Applied Cryptography", CRC Press LLC, USA XP002201307, (1997),475
		RICHT, STEFAN , et al., "In-Circuit-Emulator Wird Echtzeittauglich", Elektronik, Franzis Verlag GMBH, Munchen, DE, Vol. 40, No. 16, XP000259620,(100-103),8-6-1991
↓		ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium, XP002247347, Denver, Colorado, (8/14/00),1-17

EXAMINER

DATE CONSIDERED

10 APR 04

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> <small>(Use as many sheets as necessary)</small>		<i>Complete if Known</i>	
		Application Number	09/540613
		Filing Date	March 31, 2000
		First Named Inventor	Ellison, Carl
		Group Art Unit	Unknown
		Examiner Name	Unknown
Sheet 2 of 2			Attorney Docket No: 42P08628

**OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
SCP		SAEZ, SERGIO , et al., "A Hardware Scheduler for Complex Real-Time Systems", <u>Proceedings of the IEEE International Symposium on Industrial Electronics</u> , XP002190615,(July 1999),43-48
↓		SHERWOOD, TIMOTHY , et al., "Patchable Instruction ROM Architecture", <u>Department of Computer Science and Engineering, University of California, San Diego, La Jolla, CA</u> , (Nov. 2001),

**RECEIVED**

MAY 13 2004

Technology Center 2100

EXAMINER

DATE CONSIDERED

Substitute Disclosure Statement Form (PTO-1440)  
 \* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

LO DOL 04

## ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

StyleSheet Version v18.0

Title of Invention	Managing a Secure Environment Using a Chipset in Isolated Execution Mode
--------------------	--

Application Number: 09/540613

RECEIVED

\*09/540613\*

Confirmation Number: 2175

MAY 13 2004

First Named Applicant: Carl Ellison

Technology Center 2100

Attorney Docket Number: 42P08628

Art Unit: Unknown

Examiner: Unknown Unknown

Search string: ( 20030018892 or 4162536 or 4247905 or 4276594 or 4307447 or 4319323 or 4347565 or 4759064 or 4795893 or 4825052 or 4907270 or 4907272 or 4910774 or 5007082 or 5139760 or 5317705 or 5319760 or 5434999 or 5437033 or 5442645 or 5459867 or 5504922 or 5511217 or 5522075 or 5528231 or 5533126 or 5566323 or 5606617 or 5720609 or 5721222 or 5737604 or 5796835 or 5825875 or 5854913 or 5867577 or 5900606 or 5901225 or 5903752 or 5970147 or 6061794 or 6075938 or 6092095 or 6115816 or 6182089 or 6212635 or 6222923 or 6252650 or 6269392 or 6272637 or 6308270 or 6314409 or 6330670 or 6357004 or 6363485 or 6374286 or 6374317 or 6378072 or 6389537 or 6397242 or 6412035 or 6421702 or 6435416 or 6445797 or 6463535 or 6463537 or 6507904 or 6535988 or 6557104 or 6633963 or 6633981 ).pn.

## US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
ECT	1	20030018892	2003-01-23	Tello, Jose			
	2	4162536	1979-07-24	Morley, Richard E.			
	3	4247905	1981-01-27	Yoshida, Yukihiro , et al.		711	166
	4	4276594	1981-06-30	Morley, Richard E.			
	5	4307447	1981-12-22	Provanzano, Salvatore R., et al.			
	6	4319323	1982-03-09	Ermolovich, Thomas R., et al.			
	7	4347565	1982-08-31	Kaneda, Saburo , et al.			
	8	4759064	1988-07-19	Chaum,			
	9	4795893	1989-01-03	Ugon, Michael			
	10	4825052	1989-04-25	Chemin, Francois , et al.			
	11	4907270	1990-03-06	Hazard, Michel			

12	4907272	1990-03-06	Hazard, Michel
13	4910774	1990-03-20	Barakat, Simon
14	5007082	1991-04-09	Cummins, Mary T.
15	5139760	1994-06-07	Mason, Andrew H., et al.
16	5317705	1994-05-31	Gannon, Patrick M., et al.
17	5319760	1994-06-07	Mason, Andrew H., et al.
18	5434999	1995-07-18	Goire, Christian , et al.
19	5437033	1995-07-25	Inoue, Taro , et al.
20	5442645	1995-08-15	Ugon, Michel , et al.
21	5459867	1995-10-17	Adams, Phillip M., et al.
22	5504922	1996-04-02	Seki, Yukihiro , et al.
23	5511217	1996-04-23	Nakajima, Atsushi , et al.
24	5522075	1996-05-28	Robinson, Paul T., et al.
25	5528231	1996-06-18	Patarin, Jacques
26	5533126	1996-07-02	Hazard, Michel , et al.
27	5566323	1996-10-15	Ugon, Michel
28	5606617	1997-02-25	Brands, Stefanus A.
29	5720609	1998-02-24	Pfefferle, William C.
30	5721222	1998-02-24	Bernstein, Peter R., et al.
31	5737604	1998-04-07	Miller, David A., et al.
32	5796835	1998-08-18	Saada, Charles
33	5825875	1998-10-20	Ugon, Michel
34	5854913	1998-12-29	Goetz, John W., et al.
35	5867577	1999-02-02	Patarin, Jacques
36	5900606	1999-05-04	Rigal, Vincent
37	5901225	1999-05-04	Ireton, Mark A., et al.
38	5903752	1999-05-11	Dingwall, Thomas J., et al.
39	5970147	1999-10-19	Davis, Derek L., et al.
40	6061794	2000-05-09	Angelo, Michael E.
41	6075938	2000-06-13	Bugnion, Edouard , et al.
42	6092095	2000-07-18	Maytal, Benjamin
43	6115816	2000-09-05	Davis, Derek L.
44	6182089	2001-01-30	Ganapathy, Narayanan , et al.
45	6212635	2001-04-03	Reardon, David C.
46	6222923	2001-04-24	Schwenk, Joerg
47	6252650	2001-06-26	Nakaumra, Kouji
48	6269392	2001-07-31	Cotichini, Christian , et al.
49	6272637	2001-08-07	Little, Wendell L., et al.

50	6308270	2001-10-23	Guthery, Scott B., et al.
51	6314409	2001-11-06	Schneck, Paul B., et al.
52	6330670	2001-12-11	England, Paul , et al.
53	6357004	2002-03-12	Davis, Derek L.
54	6363485	2002-03-26	Adams, Carlisle
55	6374286	2002-04-16	Gee, John K., et al.
56	6374317	2002-04-16	Ajanovic, Jasmin , et al.
57	6378072	2002-04-23	Collins, Thomas , et al.
58	6389537	2002-05-14	Davis, Derek L., et al.
59	6397242	2002-05-28	Devine, Scott W., et al.
60	6412035	2002-06-25	Webber, Victor
61	6421702	2002-07-16	Gulick, Dale E.
62	6435416	2002-08-20	Slassi, Tarik
63	6445797	2002-09-03	McGough, Paul , et al.
64	6463535	2002-10-08	Drews, Paul C., et al.
65	6463537	2002-10-08	Tello, Jose A.
66	6507904	2003-01-14	Ellison, Carl M., et al.
67	6535988	2003-03-18	Poisner, David L.
68	6557104	2003-04-29	Vu, Son T., et al.
69	6633963	2003-10-14	Ellison, Carl M., et al.
70	6633981	2003-10-14	Davis, Derek L.

710 105

## Remarks

Note: Remarks are not for responding to an office action.

Applicants, in accordance with their duty of disclosure under 37 CFR 1.56 and in accordance with 37 CFR 1.97(b)(3), hereby submit this Electronic Information Disclosure Statement citing U.S. Patent Documents for consideration by the Examiner. Pursuant to 37 CFR 1.97, the submission of this Electronic Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability. This Electronic Information Disclosure Statement is being filed prior to a substantive examination of the claims. Pursuant to 37 CFR 1.97(b), no fee should be required for the filing of this Electronic Information Disclosure Statement. In the event it is determined that a fee is due, please charge the fee to Deposit Account 02-2666. Applicants respectfully request that the cited documents be considered and that the form be initialed by the Examiner to indicate such consideration and a copy thereof be returned to Applicants' attorney of record.

## Signature

Examiner Name	Date
Ee Lin	10 AUC '04